**Список литературы**

1. Мировой опыт развития безналичных платежных систем: ориентиры для России [Электронный ресурс]. URL: https://cyberleninka.ru/article/v/mirovoy-opyt-razvitiya-beznalichnyh-platezhnyh-sistem-orientiry-dlya-rossii.

2. Устройство и способы защиты банкомата [Электронный ресурс]. URL: https://ria.ru/infografika/20111115/489063484.html.

3. Джекпот в банкомате: зловреды и другие способы обогащения [Электронный ресурс]. URL: https://securelist.ru/malware-and-non-malware-ways-for-atm-jackpotting-extended-cut/28418/.

*4. Солем Я. Э.* Программирование компьютерного зрения на языке Python / пер. с англ. А. А. Слинкин. М. : ДМК Пресс, 2016. 312 с.

5. Рекомендации по организации комплексной централизованной охраны банковских устройств самообслуживания (Р 78.36.035–2013). М. : НИЦ «Охрана» МВД России. 2014. 203 с.

УДК 004.056

**А. В. Шаброва, Е. А. Суханова**
Научный руководитель: канд. физ.-мат. нак, доц. О. В. Ниссенбаум
Тюменский государственный университет, Тюмень

# КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ И ПРИМИТИВЫ В СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ

*Аннотация.* В статье рассмотрены криптографические протоколы и примитивы, которые могут быть использованы в сетях интернета вещей. Интернет вещей предполагает объединение в информационную сеть многих аспектов частной жизни человека и поэтому требует особой защиты. В данной работе рассматривается вопрос применимости атрибутно-основанного шифрования и легковесных криптографических примитивов в системах интернета вещей.

*Ключевые слова:* интернет вещей; атрибутно-основанное шифрование; легковесная криптография.

## Введение

В последнее время все больше внимания уделяется концепции интернета вещей (Internet of Things, IoT), который представляет собой единую информационную систему, объединяющую материальные вещи. К таким вещам относят не только привычные для Интернета устройства (компьютеры, смартфоны, сетевое оборудование), но и устройства, выполняющие специфические задачи:

умные термостаты, автомобили на самоуправлении, трекеры физической активности и другие. Как из этого следует, IoT имеет разнообразные сценарии применения, что и определяет актуальность этой концепции и повышенный к ней интерес со стороны разработчиков. В частности, объединенные сетью умные вещи могут найти применение в умных домах и городах, в управлении здоровьем, в организации транспортных сетей и прочем. Однако, каким бы ни был сценарий, умные вещи будут получать, передавать и обрабатывать критически важную для человека информацию: данные о его здоровье, жилище, привычках и передвижении. Поэтому вопрос информационной безопасности, в особенности конфиденциальности информации, обязателен для разрешения при построении интернета вещей.

**Атрибутно-основанное шифрование**

Атрибутно-основанное шифрование (Attribute-Based Encryption, ABE) было впервые описано Амитом Сахаи и Брентом Уотерсом в 2004 году [1]. Основная идея такого шифрования состоит в том, чтобы использовать атрибуты пользователя в качестве его ключа. Для генерации и выдачи ключей необходим так называемый центр выдачи атрибутов (Attribute Authority, AA). В некоторых схемах предполагается наличие нескольких центров, отвечающих за разные виды атрибутов. Такие схемы получили название Multi-Authority ABE или MA-ABE. В зависимости от того, кто определяет политику доступа к зашифрованным сообщениям, различают два возможных подхода к реализации ABE схемы: Key-Policy ABE (KP-ABE) и Ciphertext-Policy ABE (CP-ABE). В KP-ABE политика доступа включена в закрытый ключ получателя, а набор атрибутов связан с шифр-текстом. В CP-ABE политика доступа включена в шифр-текст, а набор атрибутов связан с ключом получателя. В обоих случаях через шифрование также осуществляется контроль доступа, что делает использование ABE привлекательным для Интернета вещей.

Поскольку умные вещи могут быть ограничены в вычислительных мощностях и памяти, нередко встает вопрос о фактической реализуемости ABE-схем в сетях интернета вещей. На их реализацию также влияют типы и число атрибутов, определенных политикой доступа. Так, в оригинальной CP-ABE-схеме, описанной в [2], для каждого атрибута из политики доступа необходимы две операции возведения в степень при шифровании. Расшифровывание в той же CP-ABE схеме требует $k$ возведений в степень и $2k$ билинейных отображений, в то время как в KP-ABE схеме — только $k$ билинейных отображений, где $k$ — число атрибутов, удовлетворяющих политике. Однако в [3] была продемонстрирована возможность адаптации ABE схем к использованию на таких платформах, как Raspberry Pi, Intel Galileo Gen 2 и Intel Edison.

Еще одной особенностью, которая ставит под сомнение применимость существующих ABE-схем в интернете вещей, является использование в них

билинейных отображений. Была предложена ABE-схема, основанная на эллиптических кривых, которые должны заменить тяжеловесные билинейные отображения [4]. Также использование в качестве основы алгоритма эллиптических кривых должно упростить аппаратную реализацию алгоритма, уменьшить размер зашифрованного сообщения и ключей.

Другим способом уменьшить нагрузку на конечные устройства может быть построение модели, предложенной в [5]. Эта модель предполагает наличие дополнительного полудоверенного центра (semi-trusted-authority, STA), который должен осуществлять взаимодействие с центрами выдачи атрибутов от имени пользователя, не нарушая при этом конфиденциальности ключа пользователя.

**Легковесные криптографические примитивы**

Безопасность интернета вещей непосредственно связана с используемыми в протоколах примитивами: шифрами, хеш-функциями. По большей части для таких устройств используют блочное шифрование, так как оно требует меньше ресурсов и памяти, чем асимметричные криптографические алгоритмы. Одни из известных легковесных шифров — это Present-80 и MIBS-80 и, согласно работам [6, 7], могут быть дешифрованы с вероятностью 100 % со сложностью $2^{78.98}$ и $2^{79.34}$ соответственно. Такие шифры, как Khudra и SKINNY, поддаются криптоанализу [8, 9], для полного Khudra сложность взлома — $2^{68.46}$, а для SKINNY-64-64 с 18 раундами сложность взлома — $2^{57.1}$. PRINCE [10] — блочный шифр, оптимизированный для работы в режиме реального времени, с легким внедрением в аппаратное обеспечение, на него предпринимались атаки [11], однако они не привели к полному раскрытию ключа за оптимальное время.

Таким образом, существует ряд блочных шифров, которые могут использоваться для ряда задач в области интернета вещей. Не стоит забывать, однако, о том, что в ряде случаев IoT-устройства физически доступны злоумышленнику, что делает возможным, к примеру, атаки по энергопотреблению (power attacks). Например, описана такая атака на криптографический модуль «умных ламп», работающих в режиме аутентифицированного шифрования CCM [12]. Показано, что для отдельных задач, таких как обновление прошивки, необходима асимметричная криптография, а также нужен контроль и стандартизация со стороны государства [13].

**Заключение**

Необходимость защиты конфиденциальности циркулирующей в сетях интернета вещей информации очевидна, а с развитием беспроводных сетей и ростом числа умных устройств как никогда актуальна. Между тем такие особенности IoT-систем, как большое число взаимодействующих устройств, их ограниченность в ресурсах и необходимость непрерывной работы в реальном времени требуют особого подхода в выборе и создании криптографических протоколов. Атрибутно-основанное шифрование позволяет осуществлять

контроль доступа и адресовать одно зашифрованное сообщение сразу нескольким устройствам, имеющим одинаковые наборы атрибутов, что является полезным в IoT-системах. С другой стороны, ABE-схемы должны дорабатываться, чтобы удовлетворять условию ограниченности ресурсов. Легковесные криптографические примитивы удовлетворяют этому условию, однако не все из них являются достаточно стойкими.

**Список литературы**


1. *Sahai A.*, *Waters B.* Fuzzy Identity-Based Encryption // Cryptology ePrint Archive, Report 2004/086–2004.

2. Ciphertext-Policy Attribute-Based Encryption / J. Bethencourt et al. // IEEE S&P'07–2007 .

3. On the Feasibility of Attribute-Based Encryption on Internet of Things Devices / M. Ambrosin et al. // IEEE Micro Special Issue on Internet of Things — 2016.

4. *Li F.*, *Rahulamathavan Y.*, *Rajarajan M.*, *Phan R. C.-W.* Low Complexity Multi-Authority Attribute Based Encryption Scheme for Mobile Cloud Computing // 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering. 2012. P. 573–577.

5. *Xuanxia Y.*, *Chen Z.*, *Tian Y.* A lightweight attribute-based encryption scheme for the Internet of Things // Future Generation Computer Systems, Elsevier B. V. — 2014.

6. *Abed F.*, *Forler C.*, *List E.*, *Lucks S.*, *Wenzel J.* Biclique cryptanalysis of present, led, and klein // Cryptology ePrint Archive: Report 2012/591–2012.

7. *Sereshgi F.*, *Dakhilalian M.*, *Shakiba M.* Biclique cryptanalysis of MIBS-80 and PRESENT-80 block ciphers // Security and Communication Networks. 2016. Т. 9. № 1. P. 27–33.

8. *Yang Q.*, *Hu L.*, *Sun S.*, *Song L.* Related-key impossible differential analysis of full khudra // International Workshop on Security. Springer International Publishing, 2016. P. 135–146.

9. *Tolba M.*, *Abdelkhalek A.*, *Youssef A. M.* Impossible Differential Cryptanalysis of Reduced-Round SKINNY // Cryptology ePrint Archive: Report 2016/1115–2016.

10. PRINCE — a low-latency block cipher for pervasive computing applications / Borghoff J. et al. // International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2012. P. 208–225.

11. *Rasoolzadeh S.*, *Raddum H.* Faster key recovery attack on round-reduced PRINCE // International Workshop on Lightweight Cryptography for Security and Privacy. Springer, Cham, 2016. P. 3–17.

12. *Ronen E.*, *Shamir A.*, *Weingarten A. O.*, *O'Flynn C.* IoT goes nuclear: Creating a ZigBee chain reaction // Security and Privacy (SP), 2017 IEEE Symposium on. — IEEE, 2017. P. 195–212.

13. *Shamir A.*, *Biryukov A.*, *Perrin L. P.* Summary of an Open Discussion on IoT and Lightweight Cryptography // Proceedings of Early Symmetric Crypto workshop, 2017. University of Luxembourg, 2017.

УДК 004

**М. С. Уфимцев**
Научный руководитель: канд. тех. наук, доц. А. Н. Соколов
Южно-Уральский государственный университет, Челябинск

# ИЗВЛЕЧЕНИЕ ПОБИТОВЫХ ОБРАЗОВ ФИЗИЧЕСКИХ УСТРОЙСТВ ХРАНЕНИЯ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ РАССЛЕДОВАНИЙ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Аннотация.* В работе рассматриваются основные проблемы, возникающие при извлечении побитовых образов физических устройств хранения информации. Рассмотрены возможные методы их решений. Охарактеризована правовая сторона вопроса и произведен поиск возможных критериев оценки эффективности операций по снятию образов.

*Ключевые слова:* инциденты информационной безопасности; форензика; расследование инцидентов информационной безопасности.

Специфика проведения расследовании инцидентов информационной безопасности требует максимально возможного сохранения неизменности исследуемых данных. Любой цифровой объект, с которым предстоит работать исследователю конкретного инцидента, представлен в виде компьютерной информации. Такой объект достаточно просто уничтожить, причем деструктивное воздействие может носить как умышленный, так и случайный характер.

Обеспечить полную неизменность компьютерной информации на любом носителе информации не представляется возможным за счет программно-аппаратной прослойки механизмов-посредников (работающих по принципу черного ящика) между информацией и исследователем. Примером может служить содержащийся в контроллере SSD-накопителя алгоритм ремапинга ячеек флеш-памяти, который при возникновении критических ошибок чтения/записи в ячейке сохраняет логическую структуру содержащейся в микросхеме памяти информации путем переноса сбойных ячеек в резервную область, тем самым нарушая исходную физическую структуру. В ряд этих проблем можно включить и продвинутые механизмы TRIM и garbage collection [1]. Вместо по-